Cisco Aironet 1500 Series Outdoor Mesh Access Point Hardware Installation Guide

December 2006

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-9977-05

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Aironet 1500 Series Outdoor Mesh Access Point Hardware Installation Guide

CONTENTS

Preface

This section describes the objectives, audience, organization, and conventions of the *Cisco Aironet 1500 Series Outdoor Mesh Access Point Hardware Installation Guide.*

Objectives

This publication explains the steps for installing the Cisco Aironet 1500 Series Outdoor Mesh Access Point (hereafter called the *access point*). The access point is available in two models: The LAP1510 model supports dual band (2.4- and 5-GHz) operation. The LAP1505 model supports single band (2.4 GHz) operation.

Audience

This publication is for the person installing and configuring an access point for the first time. The installer should be familiar with network structures, terms, and concepts.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Organization

This guide contains the following sections:

Chapter 1, "Overview," describes the major components and features of the access point.

Chapter 2, "Mounting Instructions," provides warnings, safety information, and mounting information needed during the installation of your access point.

Chapter 3, "Troubleshooting," provides basic troubleshooting procedures for the access point.

Appendix A, "Translated Safety Warnings," indicates how to access the document that provides translations of the safety warnings that appear in this publication.

Appendix B, "Declarations of Conformity and Regulatory Information," describes the regulatory conventions to which the access point conforms and provides guidelines for operating access points in Japan.

Appendix C, "Access Point Specifications," lists technical specifications for the access point.

Appendix D, “Channels and Power Levels,” indicates how to access the document that lists the access point radio channels and the maximum power levels supported by the world’s regulatory domains.

Appendix E, “Connector Pinouts,” describes the connector pinouts for the access point.

Appendix F, “Priming Access Points Prior to Deployment,” describes the procedure to pre-configure an access point with IP addresses and controller information.

Appendix G, “Configuring DHCP Option 43,” describes the procedure to configure DHCP Option 43.

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and keywords are in **boldface** type.

Note Means *reader take note.* Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful.* In this situation, you might do something that could result in equipment damage or loss of data.

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing

BELANGRIJKE VEILIGHEIDSINSTRUCTIES

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem **FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告　重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告　安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의　중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso　**INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel　**VIGTIGE SIKKERHEDSANVISNINGER**

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير　**إرشادات الأمان الهامة**

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.
قم بحفظ هذه الإرشادات

Upozorenje

VAŽNE SIGURNOSNE NAPOMENE

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie **WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA**

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie **DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY**

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Related Publications

These documents provide complete information about the access point:

- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*
- *Quick Start Guide: Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Points*
- *Cisco Wireless LAN Controller Configuration Guide*

Click this link to browse to the Cisco Wireless documentation home page:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

To browse to the access point documentation, click **Cisco Aironet 1500 Series** listed under "Wireless LAN Access."

To browse to the Cisco Wireless LAN Controller documentation, click **Cisco 4400 Series Wireless LAN Controllers** or **Cisco 2000 Series Wireless LAN Controllers** listed under "Wireless LAN Controllers."

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products

- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

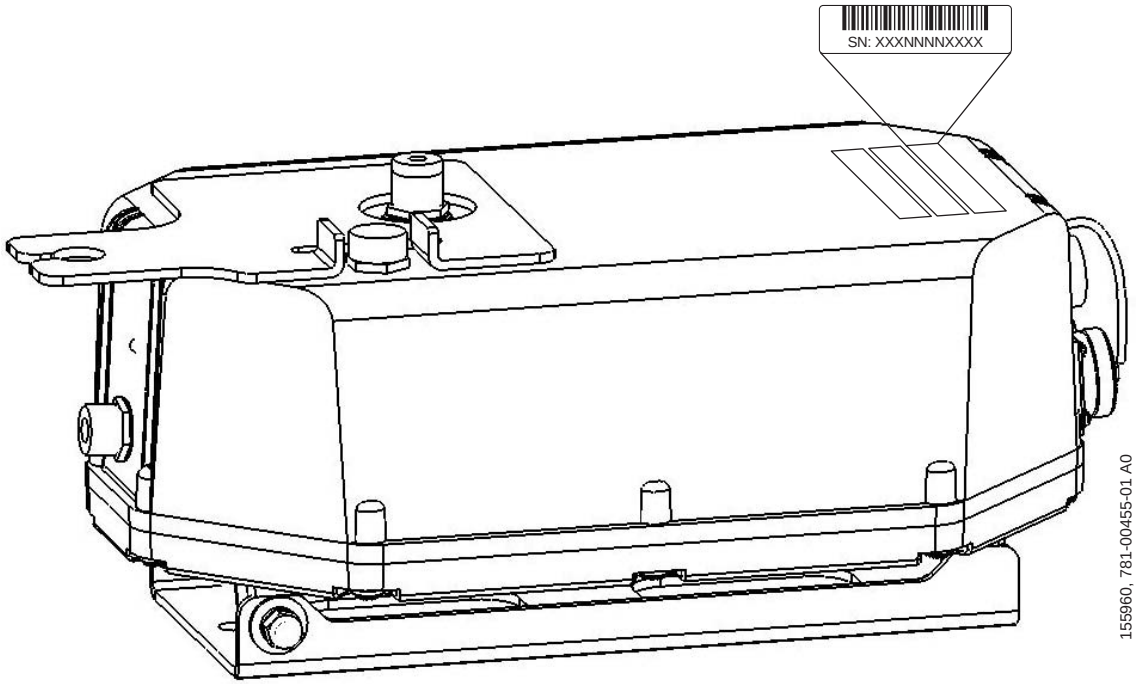
To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Finding the Product Serial Number

The access point serial number is on the right side of the housing (refer to Figure 1).

Figure 1 Location of Serial Number Label



The access point serial number label contains the following information:

- Model number, such as *AIR-LAP1510AG-A-k9* or *AIR-LAP1505G-A-k9*
- Serial number, such as *WCN0636279B* (11 alphanumeric digits)
- MAC address, such as *00abc65094f3* (12 hexadecimal digits)
- Location of manufacture, such as *Made in Singapore*

You need your product serial number when requesting support from the Cisco Technical Assistance Center.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Overview

The Cisco Aironet 1500 Series Outdoor Mesh Access Point (hereafter called the *access point*) is a wireless device designed for wireless client access, point-to-point bridging, point-to-multipoint bridging, and point-to-multipoint mesh wireless connectivity. The access point is a standalone unit that can be mounted on a streetlight pole or on a building wall or overhang.access point

The access point is available in two models: LAP1510 (supports 2.4-GHz and 5-GHz radios) and LAP1505 (supports a 2.4-GHz radio).The access point provides client access and supports 6 to 54 Mbps data rates without the need for a license. The LAP1510 model dedicates the 5-GHz radio for backhaul operations to reach a wired network and uses the 2.4-GHz radio for wireless clients. The LAP1505 model uses the 2.4-GHz radio for both backhaul and wireless clients.

The access point can also operate as a relay node for other access points not directly connected to a wired network. Intelligent wireless routing is provided by the patent-pending Adaptive Wireless Path Protocol (AWPP). This enables each access point to identify its neighbors and intelligently choose the optimal path to the wired network by calculating the cost of each path in terms of signal strength and the number of hops required to get to a controller.

The access point is configured, monitored, and operated through a Cisco wireless LAN controller (hereafter called a *controller*) as described in the *Cisco Wireless LAN Controller Configuration Guide.* The *Deployment Guide: Cisco Mesh Networking Solution* describes how to plan and initially configure the Cisco Mesh network, which supports wireless point-to-point, point-to-multipoint, and mesh deployments. The controllers use a browser-based management system, a command-line interface (CLI), or the Cisco Wireless Control System (WCS) network management system to manage the controller and the associated access points. The access point is compliant with Wi-Fi Protected Access (WPA2) and employs hardware-based Advanced Encryption Standard (AES) encryption between wireless nodes to provide end-to-end security.

This chapter provides information on the following topics:

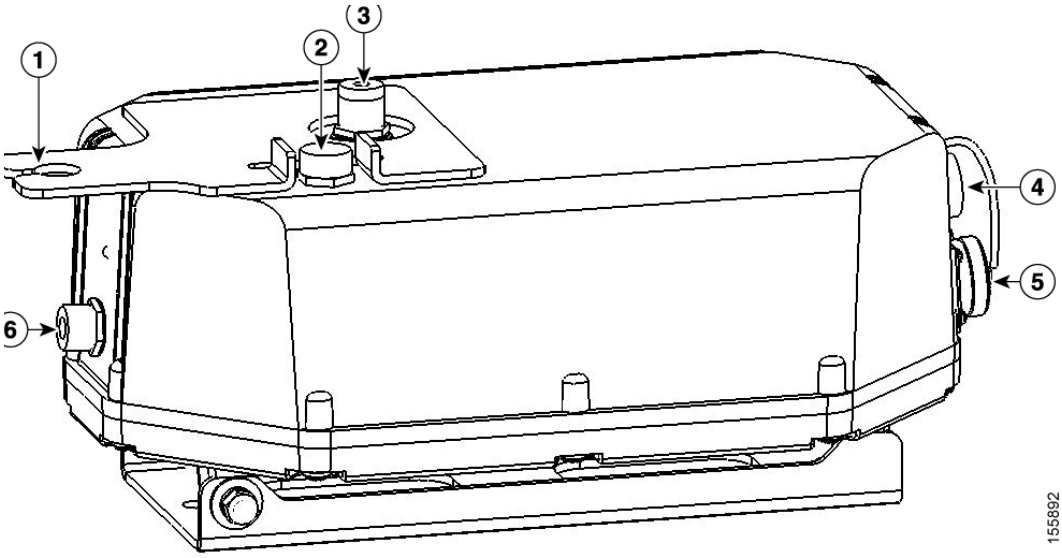
Hardware Features

Some of the access point hardware features are listed below:

- Dual simultaneous 2.4- and 5-GHz radio operation (see the "Single or Dual Radio Operation" section on page 1-3)
- External antennas (see the "External Antennas" section on page 1-3)
- Multiple power sources (see the "Multiple Power Sources" section on page 1-4)
- Ethernet port see the "Ethernet Port" section on page 1-5)
- Metal enclosure supports outdoor installations (see the "Metal Enclosure" section on page 1-6
  - Industrial temperature rating
- Optional pole mount kit (see the "Optional Hardware" section on page 1-6)
- Optional streetlight power tap adapter (see the "Optional Hardware" section on page 1-6)
- Optional 150 ft (45.72 m) Ethernet outdoor cable (see the "Optional Hardware" section on page 1-6)

Figure 1-1 shows the access point connectors.

Figure 1-1 Access Point Connectors



1	5.8-GHz antenna bracket (LAP1510 model only)	4	Ethernet (PoE) connector (MS3112P14-12P)
2	Vent (do not remove)	5	AC power connector (MS3112P14-5P)
3	2.4-GHz Type N antenna connector	6	5.8-GHz Type N antenna connector (LAP1510 model only)

Connectors

The access point supports four connectors (see Figure 1-1):

- Ethernet (PoE) connector—12 pin circular Mil spec (MS3112P14-12P)
- AC power connector—5 pin circular Mil spec (MS3112P14-5P)
- 2.4-GHz Type N antenna connector
- 5-GHz Type N antenna connector (LAP1510 model only)

Single or Dual Radio Operation

The access point is available in two models: LAP1510 (supports 2.4-GHz and 5-GHz radios) and LAP1505 (supports only a 2.4-GHz radio). The radios use external antennas (see "External Antennas").

The LAP1510 model supports simultaneous dual-radio operation using a 2.4-GHz 802.11b/g radio and a 5-GHz 802.11a radio.The 5-GHz radio incorporates an Unlicensed National Information Infrastructure (UNII) radio transceiver operating in the UNII 5-GHz frequency bands. The 5-GHz radio on the access point is used for backhaul operations to the controller. The 5-GHz radio can also operate in the 4.9-GHz Public Safety band in the United States.

Note The 4.9-GHz band requires a license and may be used only by qualified Public Safety operators as defined in section 90.20 of the FCC rules.

The LAP1505 model supports both mesh backhaul operation and wireless clients using the 2.4-GHz radio.

External Antennas

The access point is equipped with an N-type radio frequency (RF) connector on the large flat side of the unit for an external 2.4-GHz antenna. The LAP1510 model also has an N-type RF connector on the end of the unit for an external 5-GHz antenna (see Figure 1-1). When using the optional Cisco external omnidirectional antennas, the 2.4-GHz antenna connects directly to the access point, and the 5-GHz antenna connects to the access point using the antenna's included coax cable.

The Cisco omnidirectional external antennas use vertical polarization.

The access point can also be equipped with specific third-party external antennas (see Table 1-1 and Table 1-2), subject to local regulatory requirements. When you are installing third-party antennas, they must be installed with all waterproofing steps recommended by the third-party manufacturer.

Note When you mount the access point in an indoor environment, you must also mount the antennas in an indoor environment.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Table 1-1 and Table 1-2 lists the supported external antennas for the access point.

Table 1-1 External 5-GHz Antennas[1]

Part Number	Model	Gain (dBi)
AIR-ANT5175V-N	4.9 GHz Compact omnidirectional[2]	6.5
	5 GHz Compact omnidirectional	7.5
AIR-ANT58G10SSA-N	5 GHz Sector	9.5
Cushcraft S49014WP (third party)	5 GHz Patch	14
Cushcraft S54717P (third party)	5 GHz Patch	17

1. Not supported on the LAP1505 model.
2. The use of the 4.9-GHz band requires a license and may be used only by qualified Public Safety operators as defined in section 90.20 of the FCC rules.

Table 1-2 External 2.4-GHz Antennas

Part Number	Model	Gain (dBi)
AIR-ANT-2455V-N	2.4 GHz Compact Omnidirectional	5.5
Cushcraft S2406BP (third party)	2.4 GHz Omnidirectional	8

Multiple Power Sources

The access point can be powered by one of these power sources:

- 48 VDC inline power-over-Ethernet (PoE)
- AC power

Inline PoE is provided by a shielded Ethernet cable using the Cisco Aironet Power Injector (AIR-PWRINJ1500=), hereafter called the *power injector*.

Caution To provide inline PoE, you must use the power injector (AIR- PWRINJ1500=) specified for the access point. Other power injectors, PoE switches, and 802.3af power sources may not provide adequate power, which may cause the access point to malfunction and cause over-current conditions at the power source. You must ensure that the switch port connected to the access point has PoE turned off.

Caution The power injector (AIR- PWRINJ1500=) has been evaluated for installation in an indoor environment only.

Caution When the access point is installed outdoors or in a wet or damp location, the AC branch circuit that is powering the access point should be provided with ground fault protection (GFCI), as required by Article 210 of the National Electrical Code (NEC).

Note The maximum Ethernet cable length is 128 ft. (38 m) from the switch to the power injector and 200 ft. (61 m) from the power injector to the access point.

AC power is provided from an AC power source (100 to 240 VAC at 50/60 Hz):

- AC power cord options:
  - 15-ft (4.6-m) power cord (AIR-CORD1500-15NA=) for use in the US and Canada.
  - 40-ft (12.2-m) power cord (AIR-CORD1500-40NA=) for light pole installations in the US and Canada.
  - 40-ft (12.2-m) power cord (AIR-CORD1500-40UE=) for use outside the US and Canada. One end of the power cord is terminated with an access point AC power connector and the other end is unterminated.
  - 4-ft (1.2-m) streetlight power tap adapter (AIR-PWR-ST-LT-TAP=) for light pole installations in the US and Canada.

Note For important safety instructions for AC power cords, refer to the *AC Power Cords for Cisco Aironet 1500 Series Outdoor Mesh Access Points* document that shipped with your AC power cords.

Ethernet Port

The access point's Ethernet port uses a Mil-spec 12 pin connector, linking the access point to your 10BASE-T or 100BASE-T Ethernet LAN through the optional power injector. The shielded Ethernet cables are used to send and receive Ethernet data and to optionally supply inline 48-VDC power from the power injector.

The Ethernet MAC address is printed on the label on the side of the access point (refer to the "Finding the Product Serial Number" section on page xiii).

Tip The access point senses the Ethernet and power signals and automatically switches internal circuitry to match the cable connections.

Caution To provide inline PoE, you must use the power injector (AIR- PWRINJ1500=) specified for the access point. Other power injectors, PoE switches, and 802.3af power sources may not provide adequate power, which may cause the access point to malfunction and cause over-current conditions at the power source.

Metal Enclosure

The access point uses a metal enclosure that can accommodate both indoor or outdoor operating environments and an industrial temperature operating range of –40°C (–40°F) to +55°C (+131°F). The access point complies with NEMA Type 4X and IP66 requirements from IEC60529.

The access point is shipped with a mounting plate attached to the unit.

Note When the access point is mounted indoors, the antennas must also be mounted indoors.

Optional Hardware

Some of the access point hardware options are listed below:

- Pole mount kit (AIR-ACCPMK1500=)-—provides hardware for mounting the access point to the top of a metal pole, such as a streetlight pole.
- Streetlight power tap adapter (AIR-PWR-ST-LT-TAP=)—connects to the light control connector on a streetlight pole and provides AC power to the access point.
- Outdoor rated Ethernet cable (AIR-ETH1500-150=)—used to supply Ethernet and optional DC power to the access point.
- Power injector (AIR-PWRINJ1500=)—provides power-over-Ethernet (PoE) to the access point.
- AC power cord (for additional information, refer to the "Multiple Power Sources" section on page 1-4).

Network Configuration Examples

The access point is a wireless device designed for wireless client access and point-to-point bridging, point-to-multipoint bridging, and point-to-multipoint mesh wireless connectivity. The access point provides 5-GHz backhaul capability to link with another access point to reach a wired network connection or to provide repeater operations for other access points.

The access point plays two primary radio roles: a root access point (hereafter called a *RAP*) or a non-root access point (hereafter called a *MAP*). When the access point has a wired Ethernet connection to the controller (through a switch), the radio role is called a RAP. A RAP is a parent node to any bridging or mesh network. A controller can support one or more RAPs, each one parenting the same or different wireless networks. There can be more than one RAP for the same mesh network for redundancy. RAPs also support wireless clients on the band not being used for the backhaul interface.

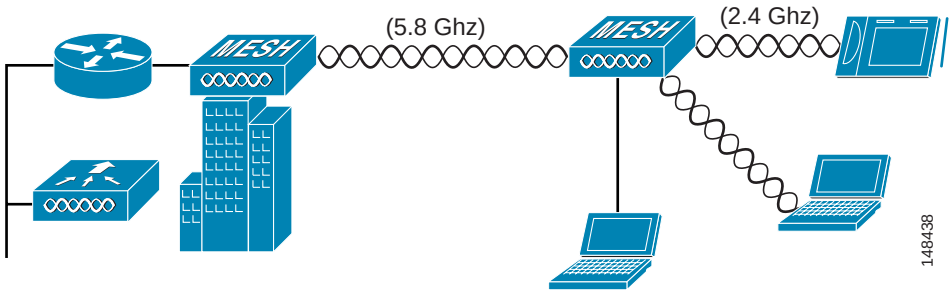
When the access point does not have a wired Ethernet connection to the controller (through a switch), the radio role is called a MAP. The MAPs have a wireless connection (through the backhaul interface) to other MAPs and finally to a RAP with an Ethernet connection through a switch to the controller. MAPs may also have a wired Ethernet connection to a local LAN and serve as a bridge endpoint for that LAN (using a point-to-point or point-to-multipoint bridge connection). MAPs also support wireless clients on the band not used for the backhaul interface.

Wireless Backhaul

The access point supports wireless backhaul capability using the 5-GHz radio to bridge to another access point to reach a wired network connection to a controller (see Figure 1-2). The access point connected to the wired network is considered a RAP in this configuration. The remote access point is considered a MAP and transfers wireless client traffic to the RAP for transfer to the wired network. Lightweight access point protocol (LWAPP) control traffic is also transferred over this bridged link.

Note The LAP 1505 model uses the 2.4-GHz radio for backhaul and wireless client operations.

Figure 1-2 Access Point Backhaul Example



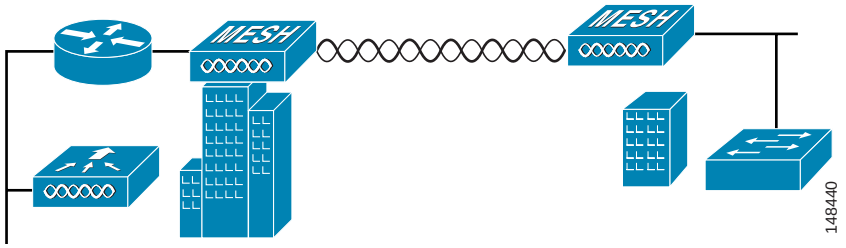
Point-to-Point Bridging

The access points can be used to extend a remote network by using the 5-GHz backhaul radio to bridge the two network segments as shown in Figure 1-3. To support Ethernet bridging, you must enable bridging on the controller for each access point.

Note The LAP 1505 model uses the 2.4-GHz radio for bridging operations.

Wireless client access is supported; however, if bridging between tall buildings, the 2.4-Ghz wireless coverage area may be limited and possibly not suitable for direct wireless client access.

Figure 1-3 Access Point Point-to-Point Bridging Example

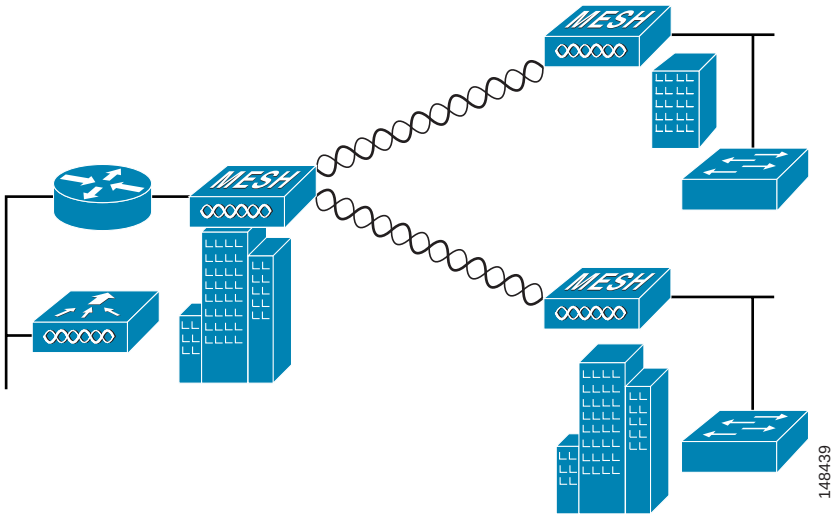


Point-to-Multipoint Bridging

The access points can be used as a RAP to connect multiple remote MAPs with their associated wired networks (see Figure 1-4). By default this capability is turned-off for all access points. To support Ethernet bridging, you must enable bridging on the controller for each access point.

Wireless client access can be provided over the bridging link; however, if bridging between tall buildings, the 2.4-Ghz wireless coverage area may be limited and possibly not suitable for direct wireless client access.

Figure 1-4 Access Point Point to Multipoint Bridging Example



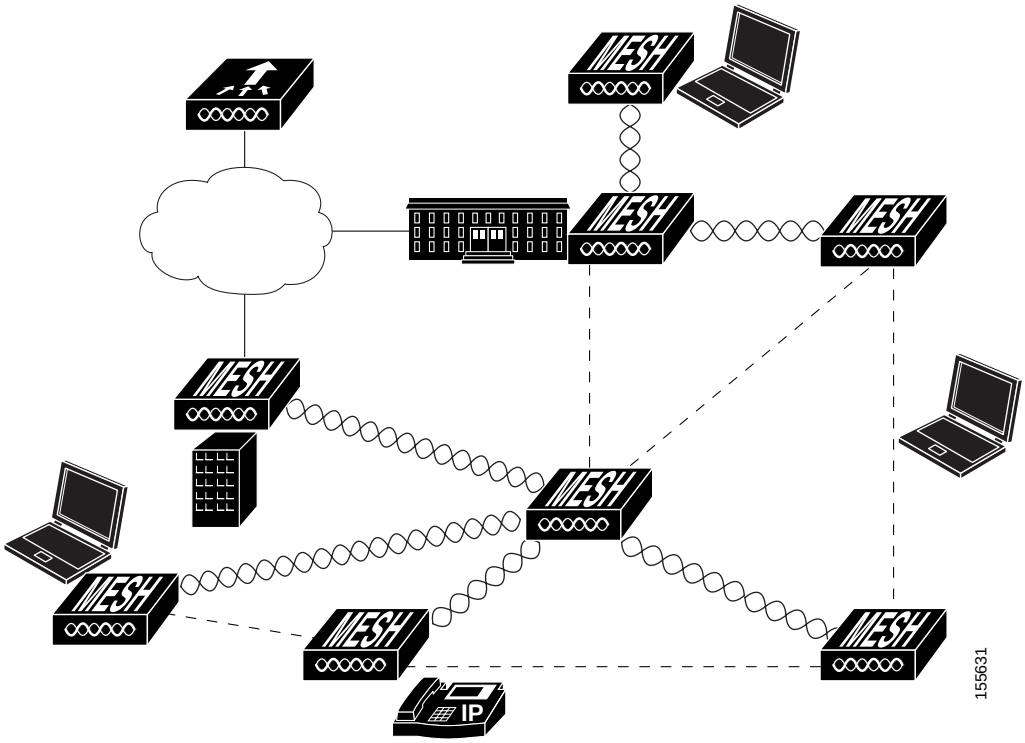
Mesh Network

The access points are typically deployed in a mesh network configuration. In a typical mesh deployment, one or more RAPs have a wired network connection through a switch to a controller. Other remote MAPs without wired network connections use the backhaul feature to optimally link to a RAP that is connected to the wired network. In the mesh network, the links between the access points are referred to as the *backhaul links*.

Intelligent wireless routing is provided by the patent-pending Adaptive Wireless Path protocol (AWPP). This enables each MAP to identify its neighbors and intelligently choose the optimal path to the RAP with the wired network connection by calculating the cost of each path in terms of signal strength and the number of hops required to get to a controller.

Figure 1-5 illustrates a typical mesh configuration using MAPs and RAPs.

Figure 1-5 Typical Mesh Configuration Using Access Points



Layer 2 and Layer 3 Network Operation

The access points support Layer 2 or Layer 3 network operation. In Layer 2 configurations, the access point and the controller are on the same subnet and communicate with encapsulated Ethernet frames using MAC addresses rather than IP addresses. Layer 2 configurations are typically not scalable into larger networks. Additionally, Layer 2 operation is supported only by the Cisco 4400 series controllers.

Access points and controllers in Layer 3 configurations use IP addresses and UDP packets, which can be routed through large networks. Layer 3 operation is scalable and recommended by Cisco.

Figure 1-6 illustrates a typical Layer-3 wireless network configuration containing access points and a controller.

Figure 1-6 Typical Layer 3 Access Point Network Configuration Example

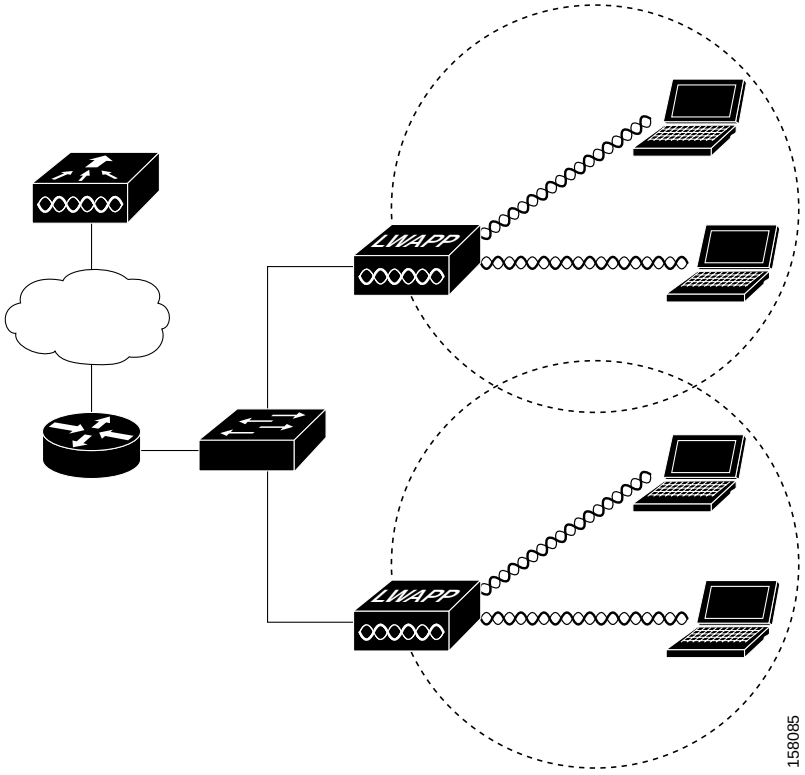
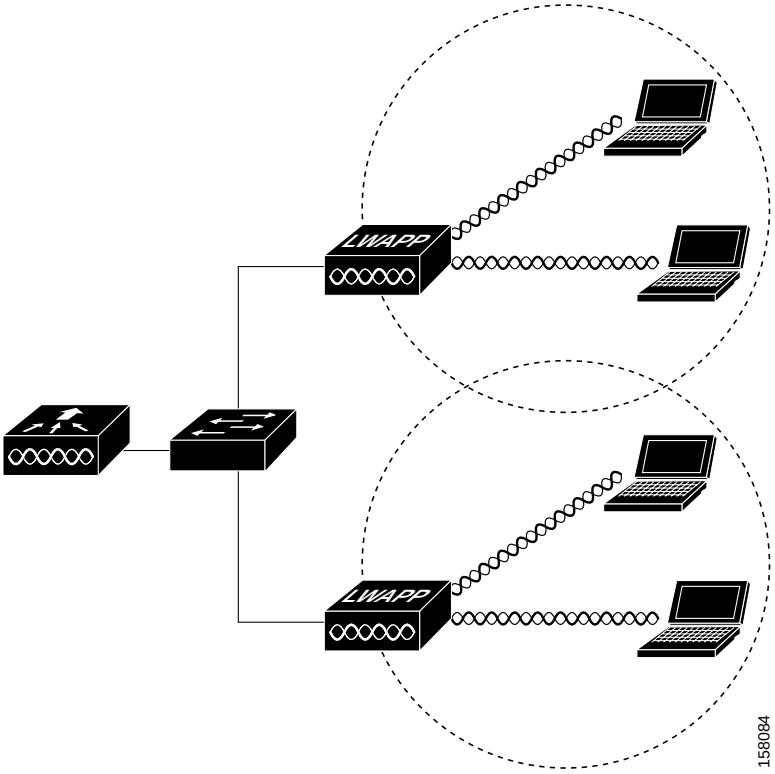


Figure 1-7 illustrates a typical Layer 2 network configuration. In a Layer 2 configuration, the controller and the access points are on the same subnet.

Figure 1-7 Typical Layer 2 Access Point Network Configuration Example



CHAPTER 2

Mounting Instructions

This chapter describes warnings, safety information, and mounting information needed during the installation of your access point. The chapter contains these sections:

Unpacking the Access Point

Note When you are unpacking the access point, do not remove the foam blocks attached to the antenna connectors. The foam protects the antenna connectors during installation.

Follow these steps to unpack the access point:

Step 1 Open the shipping container and carefully remove the contents.

Step 2 Return all packing materials to the shipping container and save it.

Step 3 Ensure that all items listed in Package Contents are included in the shipment. If any item is damaged or missing, notify your authorized Cisco sales representative.

Package Contents

Each access point package contains the following items:

- Access point with mounting plate attached
- Cisco product documentation, translated safety warnings, registration and feedback cards
- Grounding lug with screw and lock washer

Tools and Materials

To install the access point you will need the following:

- Open and box-end wrenches or socket set and ratchet
- Customer-supplied 10-AWG copper ground wire
- Ground lug (Panduit PN-10-6R-2K) and screw with lock washer (supplied)
- Customer supplied crimping tool for the ground lug (Panduit PN-10-6R-2K)
- Optional power injector (AIR-PWRINJ1500=)
- Optional Ethernet cable
  - 150-ft (45.72-m) Ethernet cable (AIR-ETH1500-150=)
  - Other lengths (user supplied)
- Optional AC power cord
  - 15-ft (4.6-m) power cord (AIR-CORD1500-15NA=) for use in the US and Canada.
  - 40-ft (12.2-m) power cord (AIR-CORD1500-40NA=) for light pole installations in the US and Canada.
  - 40-ft (12.2-m) power cord (AIR-CORD1500-40UE=) for use outside the US and Canada. One end of the power cord is terminated with an access point AC power connector and the other end is unterminated.

  - 4-ft (1.2-m) streetlight power tap adapter (AIR-PWR-ST-LT-TAP=) for light pole installations in the US and Canada.
- Optional pole mount kit (AIR-ACCPMK1500=)
- External antennas, 2.4 and 5 GHz (refer to the "External Antennas" section on page 1-3)
- Optional primary protector (user supplied), as required by local regulations
- Optional ladder, power lift, rope, or other tools as required

Warnings

Translated versions of all safety warnings are available in the safety warning document that shipped with your access point or on Cisco.com. To browse to the document on Cisco.com, refer to Appendix 1, "Translated Safety Warnings" for instructions.

Warning **IMPORTANT SAFETY INSTRUCTIONS**
This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071
SAVE THESE INSTRUCTIONS

Warning **Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 364

Warning **This equipment must be externally grounded using a customer-supplied ground wire before power is applied. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 366

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the access point.

FCC Safety Compliance Statement

The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

Warning **In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft (2 m) from your body or nearby persons.** Statement 339

Warning **The AC power supply has double pole/neutral fusing.** Statement 188

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **This equipment has been designed for connection to TN and IT power systems.** Statement 1007

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, because they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (for example, U.S.:NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54).** Statement 1052

Caution No serviceable parts inside. Do not open.

Caution Double pole/neutral fusing. The power supply has two fuses and might have live circuits even when one fuse has blown.

Note For additional important safety instructions for AC power cords, refer to the *AC Power Cords for Cisco Aironet 1500 Series Outdoor Mesh Access Points* document that shipped with your AC power cords.

Each year hundreds of people are killed or injured when attempting to install an antenna. In many of these cases, the victim was aware of the danger of electrocution, but did not take adequate steps to avoid the hazard.

For safety, and to help you achieve a good installation, please read and follow these safety precautions. They may save your installer's life!

1. Select your installation site with safety, as well as performance in mind. Remember: electric power lines and phone lines look alike. For safety, assume that any overhead line can kill.
2. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your installer's life is at stake.
3. Plan your installation carefully and completely before you begin. Successful raising of a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task, and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
4. When installing the access point and antennas, remember:
   a. Do not use a metal ladder.
   b. Do not work on a wet or windy day.
   c. Do dress properly—shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
5. Use a rope to lift the access point. If the assembly starts to drop, get away from it and let it fall.
6. If any part of the antenna system should come in contact with a power line, don't touch it or try to remove it yourself. Call your local power company. They will remove it safely.

If an accident should occur call for qualified emergency help immediately.

Avoiding Damage to Radios in a Testing Environment

The radios on outdoor units (bridges) have higher transmit power levels than radios on indoor units (access points). When you test high power radios in a link, you must avoid exceeding the receiver's maximum receive input level. At levels above normal the operating range, packet error rate (PER) performance is degraded. At even higher levels, the receiver can be permanently damaged. To avoid receiver damage and PER degradation, you can use one of the following techniques:

- Separate the omnidirectional antennas by at least 2 ft (0.6 m) to avoid receiver damage or by at least 25 ft (7.6 m) to avoid PER degradation.

Note These distances assume free space path loss and are conservative estimates. Required separation distances for damage and performance degradation levels in actual deployments will be less due to non line-of-sight propagation conditions.

- Reduce the configured transmit power to the minimum level.
- Use directional antennas and keep them away from each other.
- Cable the radios together using a combination of attenuators, combiners, or splitters to achieve a total attenuation of at least 60 dB.

For a radiated test bed, the following equation describes the relationships among transmit power, antenna gain, attenuation, and receiver sensitivity:

```
txpwr + tx gain + rx gain - [attenuation due to antenna spacing] < max rx input level
Where:
txpwr = Radio transmit power level
tx gain = transmitter antenna gain
rx gain = receiver antenna gain
```

For a conducted test bed, the following equation describes the relationships among transmit power, antenna gain, and receiver sensitivity:

```
txpwr - [attenuation due to coaxial components] < max rx input level
```

Caution Under no circumstances should you connect the antenna port from one access point to the antenna port of another access point without using an RF attenuator. If you connect antenna ports you must not exceed the maximum survivable receive level of 0 dBm. Never exceed 0 dBm or damage to the access point can occur. Using attenuators, combiners, and splitters having a total of at least 60 dB of attenuation ensures that the receiver is not damaged and PER performance is not degraded.

Installation Guidelines

Because the access point is a radio device, it is susceptible to common causes of interference that can reduce throughput and range. Follow these basic guidelines to ensure the best possible performance:

- For information on planning and initially configuring your Cisco Mesh network, refer to the *Deployment Guide: Cisco Mesh Networking Solution.*
- Perform a site survey before beginning the installation.
- Install the access point in an area where structures, trees, or hills do not obstruct radio signals to and from the access point.
- The access points can be installed at any height, but best throughput is achieved when all the access points are mounted at the same height.

Note Cisco recommends installing the access points no higher than 40 feet to allow support for wireless clients on the ground.

Note To calculate path loss and to determine how far apart to install access points, consult an RF planning expert.

Site Surveys

Every network application is a unique installation. Before installing multiple access points, you should perform a site survey to determine the optimum use of networking components and to maximize range, coverage, and network performance.

Consider the following operating and environmental conditions when performing a site survey:

- Data rates—Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver sensitivity occurs as the radio data increases.

- Antenna type and placement—Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height. However, do not place the antenna higher than necessary, because the extra height also increases potential interference from other unlicensed radio systems and decreases the wireless coverage from the ground.
- Physical environment—Clear or open areas provide better radio range than closed or filled areas.
- Obstructions—Physical obstructions such as buildings, trees, or hills can hinder performance of wireless devices. Avoid locating the devices in a location where there is an obstruction between the sending and receiving antennas.

Before Beginning the Installation

Before you begin the installation process:

- Ensure that a site survey has been performed.
- Ensure that your network infrastructure devices are operational and properly configured.
- Ensure that your controllers are connected to switch trunk ports.
- Ensure that your switch is configured with untagged access ports for connecting your access points.
- Ensure that a DHCP server with Option 43 configured is reachable by your access points or manually configure the controller information in the access point (for additional information, refer to the "Configuring DHCP Option 43" section on page G-1).
- Become familiar with the access point installation components (see the "Becoming Familiar with Access Point Installation Components" section on page 2-7).
- Add the MAC addresses of the access points to the controller's filter list (see the "Adding the Access Point MAC Addresses to the Controller Filter List" section on page 2-10).
- Enable automatic configuration of access points on the controller (see the "Enabling Zero Touch Configuration on the Controller" section on page 2-10).

Becoming Familiar with Access Point Installation Components

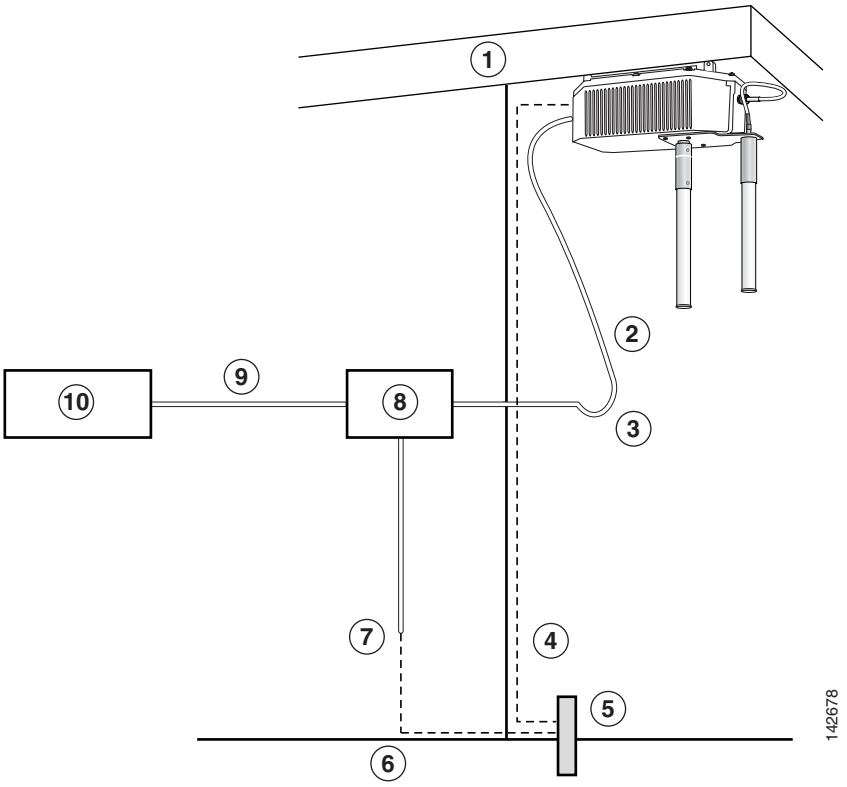
The access point is designed to be installed in an indoor or outdoor environment, such as an interior wall or ceiling or the exterior roof overhang of a tall building or a streetlight pole.

Note When you mount access point in an indoor environment, you must also mount the attached antennas in an indoor environment.

Carefully review the following figures to become familiar with the system components, connectors, indicators, cables, system interconnection, and grounding:

- Components in a Typical Access Point Installation (Figure 2-1)
- Access point connectors (Figure 2-2)
- Streetlight power tap installation (Figure 2-3)

Figure 2-1 Components in a Typical Access Point Installation



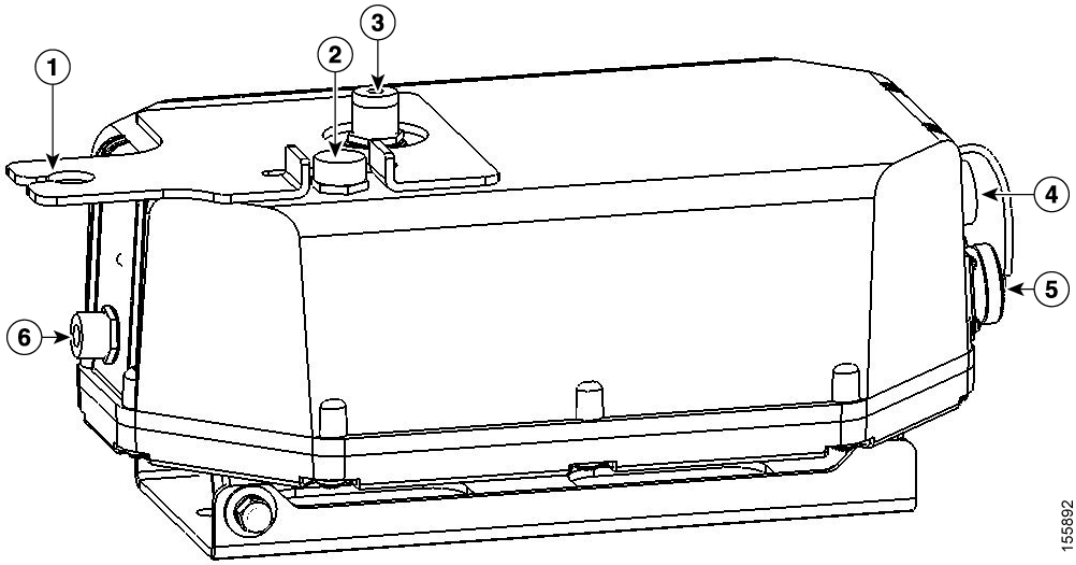
1	Building roof-overhang	**6**	Ground
2	Outdoor rated shielded Ethernet cable[1]	**7**	AC power cord[2]
3	Water drip loop	**8**	Power injector[3]
4	10-AWG copper grounding wire[1]	**9**	Ethernet (CAT 5) cable[1]
5	Ground rod[1]	**10**	Controller (through a switch)

1. User supplied.
2. The safety ground wire in the AC power cord must have a ground path to a grounding rod.
3. The shielded Ethernet cable has a ground path through the power injector and the safety ground wire in the AC power cord.

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

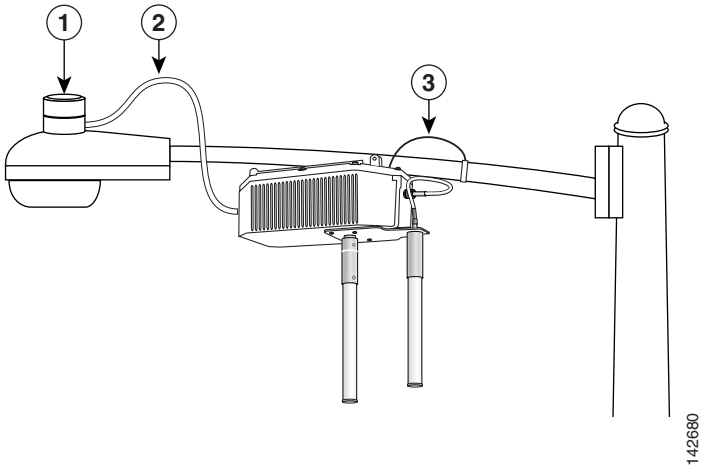
Note There is no requirement for external lightening arrestors on the 1510. The power supplies on the 1510 and the PoE in ports have transient voltage surge suppression. In addition, the PoE in port should be used with shielded cables that are grounded at the access point and power injector.

Figure 2-2 Access Point Connectors



1	5.8-GHz antenna bracket (LAP1510 model)	**4**	Ethernet (PoE) connector (MS3112P14-12P)
2	Vent (do not remove)	**5**	AC power connector (MS3112P14-5P)
3	2.4-GHz antenna connector (Type-N)	**6**	5.8-GHz Type N antenna connector (LAP1510 model)

Figure 2-3 Streetlight Power Tap Adapter Installation



1	Outdoor light control	**3**	10-AWG copper grounding wire
2	Streetlight power tap adapter		

Adding the Access Point MAC Addresses to the Controller Filter List

Prior to installing your access points, configure your controller by adding the MAC addresses of the access points to the filter list and enable Zero Touch Configuration. This enables the controller to respond to the listed access points and transfer the Bridge Shared Secret Key to each access point. The secret key is required for the access points to communicate with other access points in the same bridge group upon installation. Follow these steps to add a MAC filter entry on the controller:

Step 1 Log into your controller using a web browser.

Step 2 Choose **SECURITY > MAC Filtering > New**.

Step 3 Enter the MAC address of the access point to the MAC Filter list; for example, *00:0B:91:21:3A:C7*.

Step 4 Select a WLAN ID or **Any WLAN** from the WLAN ID pop-up menu.

Step 5 Enter a description (32 characters maximum) of the access point in the Description field; for example, *Fisher_Street_00.0B.91.21.3A.C7* shows the location and MAC address of the access point.

Step 6 Choose an interface from the Interface Name pop-up menu and click **Apply**.

Step 7 Repeat Steps 2 to 6 to add other access points to the list.

Step 8 Log out of your controller and close your web browser.

Enabling Zero Touch Configuration on the Controller

Follow these steps to enable automatic configuration of access points on the controller:

Step 1 Log into your controller using a web browser.

Step 2 Choose **WIRELESS > MESH**.

Step 3 Check **Enable Zero Touch Configuration**.

Note If you do not specify a new bridging shared secret key and key format, the default or the existing configured value is used.

Step 4 [Optional] Choose a key format by clicking the down arrow in the Key Format field.

Step 5 [Optional] Enter a new secret key and confirm the entry.

Step 6 Click **Apply**.

Note You can also use the controller CLI command **config network zero-config** to enable automatic configuration.

Step 7 Log out from your controller and close your web browser.

Configuring a RAP

The access point defaults to the MAP radio role. One or more of your access points must be reconfigured as a RAP. The RAPs connect to a wired Ethernet link through a switch to the controller. The MAPs use their wireless backhaul interface to connect to a RAP to reach the controller.

Follow these steps to configure a RAP on the controller:

Step 1 Log into your controller using a web browser.

Step 2 Click **Wireless**. When your access point associates to the controller, your access point's name is visible in the AP Name list.

Step 3 Find your access point's name and click **Detail**.

Step 4 Find Bridging Instructions and choose **Root AP** by clicking the drop down arrow in the AP Role field.

Step 5 Click **Apply**.

Step 6 Repeat Steps 2 through 5 for each RAP.

Step 7 Log out from your controller and close your web browser.

Mounting the Access Point

This section provides instructions for installing your access points. Personnel installing the access point must understand wireless access points and bridging techniques and grounding methods.

Installation Options

There are two common installation methods: a roof-overhang or wall installation using the access point mounting plate (supplied) or a pole installation using the optional pole mount kit.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

Caution When the product is installed outside of the building, and the DC power/Ethernet connection is used, this cabling should be installed in accordance with the requirements of a Class 2 circuit, as detailed in Article 725 of the National Electric Code (NEC). Such requirements include, but are not limited to, routing the Class 2 cabling away from AC power lines and AC building wiring, and limiting the exposed cable runs external to the building to less than 140 ft (42m) – or is directly buried or in underground conduit, where a continuous metallic cable shield or a continuous metallic conduit containing the cable is bonded to each building grounding electrode system. If such installation methods are not followed, the cabling must be installed according to the requirements for telecommunication circuits (TNV) as detailed in

Article 800, which includes requirements for a Listed primary protector upon entering the building, and limits the installation to only Listed networking equipment designed to accommodate telecommunication interfaces.

Caution To provide inline PoE, you must use the power injector (AIR- PWRINJ1500=) specified for the access point. Other power injectors, PoE switches, and 802.3af power sources may not provide adequate power, which may cause the access point to malfunction and cause over-current conditions at the power source. You must ensure that the switch port connected to the access point has PoE turned off.

Refer to these sections for installation details.

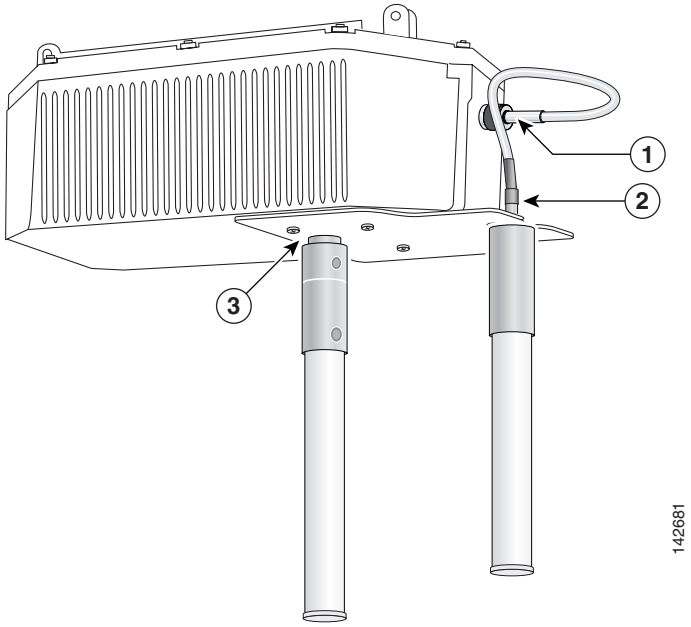
- Access Point Mounting Orientations, page 2-12
- Mounting the Access Point on a Vertical or Horizontal Surface, page 2-15
- Roof-Overhang Installation, page 2-16
- Mounting the Access Point on a Pole, page 2-17
- Streetlight Pole Installations, page 2-21

Access Point Mounting Orientations

When installing an access point on a horizontal or vertical surface, you must ensure that the access point is correctly oriented.

Caution When mounting the access point in a horizontal position, you must position the side with the 2.4-GHz antenna connector facing down (see Figure 2-4). When you are mounting the access point in a vertical position, you must position the access point with the 5-GHz antenna connector facing up (see Figure 2-5). This positioning is required to prevent water intrusion into the unit from the vent. You must ensure that the vent is not obstructed by anything.

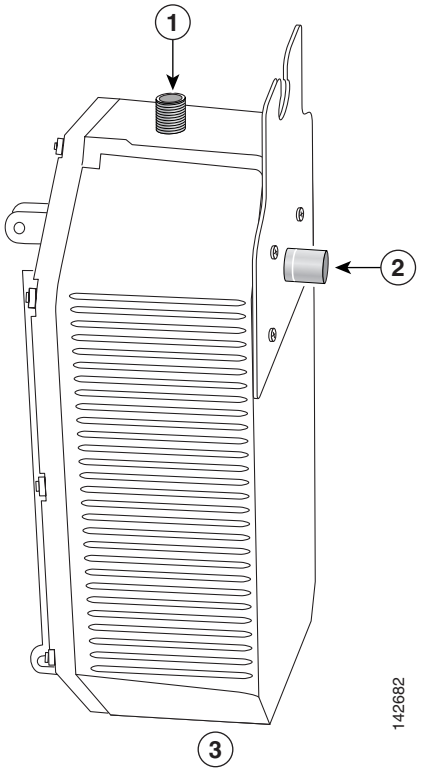
Figure 2-4 Preferred Horizontal Orientation



1	5-GHz antenna connector (LAP1510 model)	**3**	2.4-GHz antenna connector (this side down)
2	5-GHz antenna cable (LAP1510 model)		

Figure 2-5 illustrates the access point vertical orientation.

Figure 2-5 Optional Vertical Orientation



1	5-GHz external antenna connector (LAP 1510 model)	**3**	This end must be down
2	2.4-GHz external antenna connector		

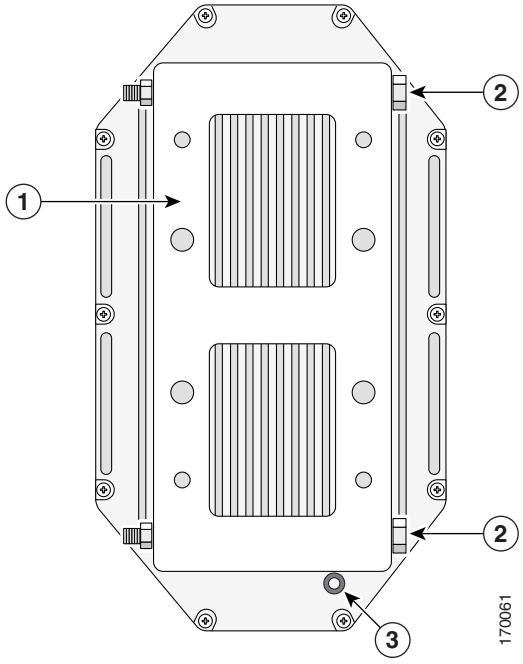
Note Omnidirectional antennas must be mounted vertically.

Mounting the Access Point on a Vertical or Horizontal Surface

To mount the access point on a vertical or horizontal surface such as a wall or a roof-overhang, use the supplied mounting plate. For the correct access point mounting orientations, refer to the "Access Point Mounting Orientations" section on page 2-12.

Step 1 The mounting plate is attached to the access point by two carriage bolts. Refer to Figure 2-6 for the location of the carriage bolts securing the mounting plate.

Figure 2-6 Access Point Mounting Plate and Carriage Bolts



1	Mounting plate	**3**	Grounding screw hole
2	Carriage bolts		

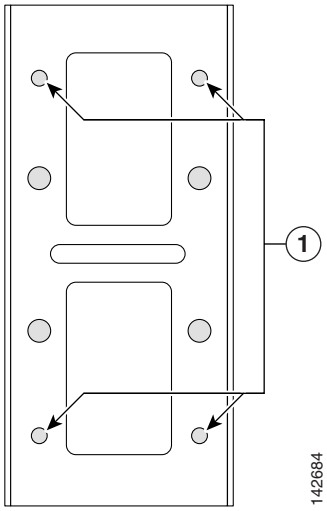
Step 2 Remove the nuts and washers from the carriage bolts and remove the carriage bolts.

Step 3 Remove the mounting plate from the access point.

Step 4 Use the mounting plate as a template to mark four screw hole locations on your mounting surface. See Figure 2-7 for the mounting plate screw hole locations.

Caution The mounting surface, attaching screws, and optional wall anchors must be able to support a 50 lbs (22.7 kg) static weight.

Figure 2-7 Mounting Plate Screw Hole Locations



1	Four locations		

Step 5 Use four customer-supplied screws and optional screw anchors to attach the mounting plate to the mounting surface.

Note If necessary, use suitable screw anchors and an exterior-grade plywood backboard to mount the access point to stucco, cement, or drywall.

Step 6 Use the carriage bolts and the associated nuts and washers to reattach the access point to the mounting plate. Tighten the nuts to 61 to 71 in. lbs (6.89 to 8.02 Nm).

Step 7 Continue with the "Roof-Overhang Installation" section.

Roof-Overhang Installation

When your access point is mounted on a roof overhang, follow these steps to complete the installation:

Step 1 Review Figure 2-1 to identify the components needed for the installation.

Step 2 Connect a Category 5 Ethernet cable from your wired LAN network to the optional power injector.

Caution When the product is installed outside of the building, and the DC power/Ethernet connection is used, this cabling should be installed in accordance with the requirements of a Class 2 circuit, as detailed in Article 725 of the National Electric Code (NEC). Such requirements include, but are not limited to, routing the Class 2 cabling away from AC power lines and AC building wiring, and limiting the exposed cable runs external to the building to less than 140 ft (42 m) – or is directly buried or in underground conduit, where a continuous metallic cable shield or a continuous metallic conduit containing the cable is bonded to each building grounding electrode system. If such installation methods are not used, the cabling must be installed according to the requirements for telecommunication circuits (TNV) as detailed in Article 800, which includes requirements for a Listed primary protector upon entering the building, and limits the installation to only Listed networking equipment designed to accommodate telecommunication interfaces.

Use only the specified power injector (AIR-PWRINJ1500=) for the access point. This power injector is designed to meet the power requirements of the access point and is a listed Class 2 Limited Power Source (LPS).

Tip To forward bridge traffic, add a switch between the power injector and controller. Refer to the *Deployment Guide: Cisco Mesh Networking Solution* for more information.

Step 3 Ensure the antennas are connected to the access point before you apply power to the access point.

Step 4 Connect a shielded outdoor-rated Ethernet cable (such as AIR-ETH1500-150=) between the power injector and the access point's Ethernet connector (see Figure 2-2).

Note You should hand-tighten the access point Ethernet cable connector until the connector locks.

Warning **Use the captive connector cap on the unused mil spec connector to prevent water intrusion and possible safety hazards.** Statement 362

Step 5 When using the optional Cisco external omnidirectional antennas, connect them to the access point as shown in Figure 2-1. When using other Cisco external antennas, mount them as directed by the installation documentation that shipped with the antennas.

Step 6 When using optional third-party external antennas, mount and connect them as described in the installation documents that shipped with the antennas.

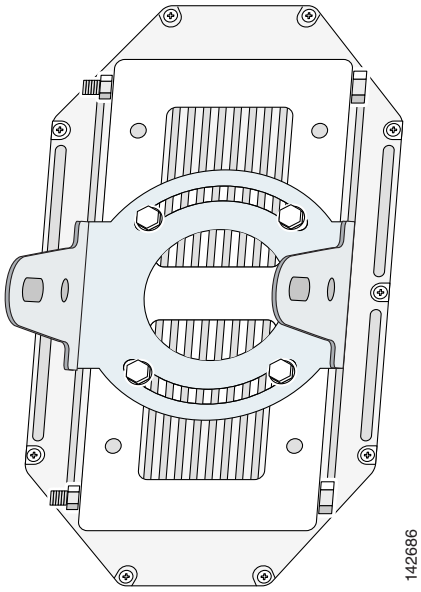
Step 7 Continue with the "Grounding the Access Point" section on page 2-21.

Mounting the Access Point on a Pole

When installing an access point on a pole or mast, you should use the optional Cisco pole mount kit. To mount the access point on a pole, perform these steps:

Step 1 From the pole mount kit, use four of the supplied short bolts, lock washers, and flat washers to attach the pole mount kit adjustment plate to the access point mounting plate as shown in Figure 2-8. Tighten the bolts to 15 to 20 ft. lbs. (20 to 27 Nm).

Figure 2-8 Adjustment Plate Attached to the Mounting Plate

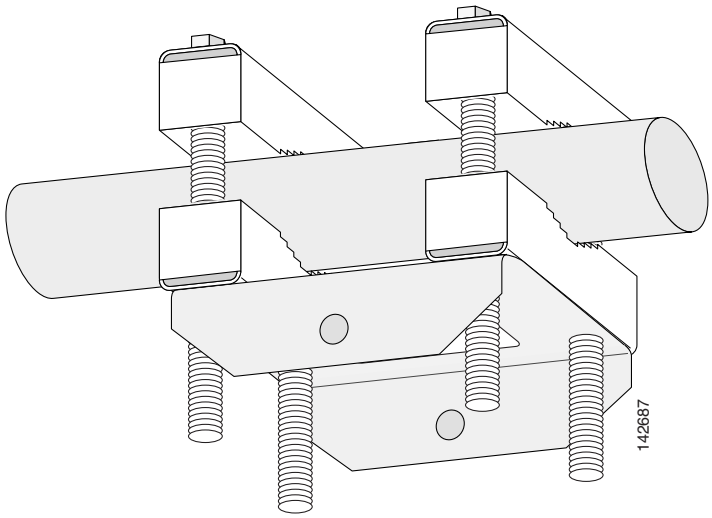


Step 2 Select a mounting location. You can attach the access point to any pole from 1.66 to 3.35 in. (4.22 to 9.02 cm) in diameter.

Note If you will be using a streetlight power tap adapter, position the access point within 3 ft (1 m) of the outdoor light control.

Step 3 Loosely assemble the pole clamp components around the pole and thread the four long bolts into the clamp adjustment plate. Figure 2-9 shows the pole clamp attached to a pole with the clamp adjustment plate positioned on the bolts.

Figure 2-9 Pole Clamp and Clamp Adjustment Plate Mounted on a Pole



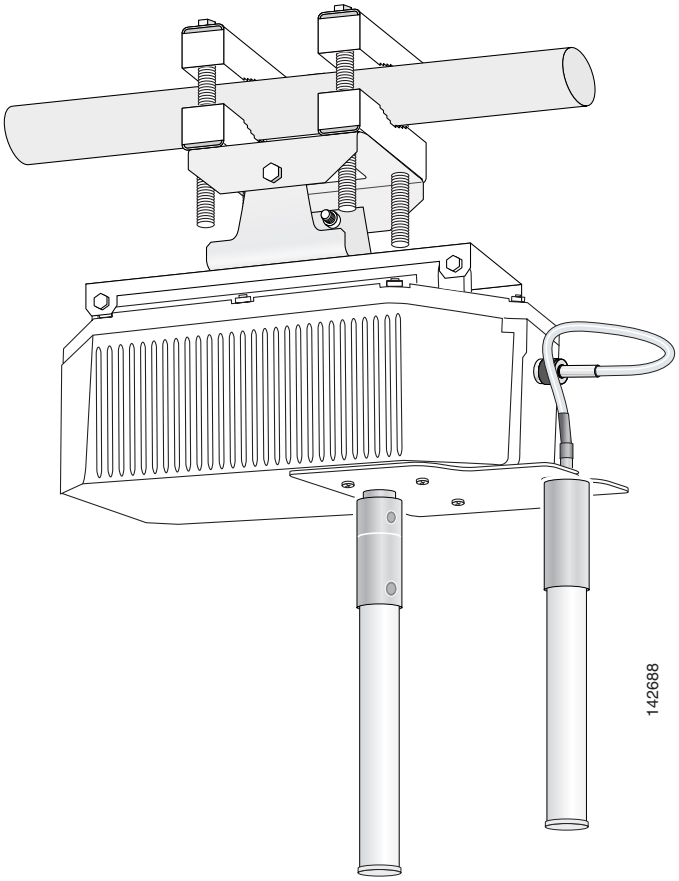
Step 4 Adjust the top edge of the pole clamp until it is horizontal and tighten the bolts to 15 to 20 ft. lbs. (20 to 27 Nm)

Note If you need longer bolts, purchase 3/8–16 bolts of the correct length for your installation. Also, the bolts can protrude up to 2 in (5 cm) and still allow the pole mount assembly to swivel and rotate.

Step 5 From the pole mount kit, use the two short bolts, lock washers, and flat washers to loosely attach the two adjustment plates as shown in Figure 2-10.

Note Do not over-tighten the bolts. You will need to adjust the access point orientation.

Figure 2-10 Access Point Attached to the Pole Clamp



Step 6 If necessary, rotate the access point until the top edge of the housing is horizontal, and tighten the two short bolts on the adjustment plates. Torque the bolts to 15 to 20 ft. lbs. (20 to 27 Nm).

Step 7 Continue with the "Grounding the Access Point" section on page 2-21.

Grounding the Access Point

Warning **This equipment must be externally grounded using a customer-supplied ground wire before power is applied. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 366

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

In all outdoor installations and when powering the access point with AC power, you must follow these instructions to properly ground the case:

Step 1 If using insulated 10-AWG copper ground wire, strip the insulation as required for the grounding lug.

Step 2 Use the appropriate crimping tool to crimp the bare 10-AWG copper ground wire to the grounding lug (Panduit PN-10-6R-2K lug supplied).

Step 3 Connect the grounding lug to the access point grounding screw hole using the supplied Phillips head screw (6-32x1/4 stainless steel) with lock washer (McMaster-Carr 95345A458 or equivalent). The grounding screw hole is located on the mounting plate side of the access point case near the 5-GHz antenna connector (see Figure 2-6). Tighten the grounding screw to 7 to 8 in. lbs. Do not overtighten!

Step 4 If necessary, strip the other end of the ground wire and connect to a reliable earth ground, such as a grounding rod or an appropriate grounding point on a metal streetlight pole that is grounded (see Figure 2-1 and Figure 2-11).

Streetlight Pole Installations

The access point can be installed where power is available, without the need for a wired LAN connection. The access point uses intelligent wireless routing that is based on the Adaptive Wireless Path Protocol (AWPP). AWPP enables a remote access point to dynamically optimize the best route to the wired LAN network using another access point.

The LAP1510 model uses the 5-GHz radio for the Mesh backhaul Mesh connections. The 2.4-GHz radio is used for local wireless client access. The LAP1505 model uses the 2.4-GHz radio for both Mesh backhaul and local wireless client access.

The access point can be installed on a streetlight pole and powered from a streetlight outdoor light control using the optional streetlight power tap adapter.

Caution The access point can be powered by a light pole twist-lock outdoor light control that provides 100- to 240-VAC 50/60 Hz power. Do not connect to an outdoor light control powered by higher voltages.

When powering the access point with AC power other than the streetlight power tap adapter, you must ensure that the following conditions are observed:

1. AC power can be conveniently removed from the unit. The power should not be removed by disconnecting the AC power connector on the unit.

Caution A readily accessible service disconnect device must be incorporated in the fixed wiring. The disconnect device must open all of the phase conductors.

2. You must protect any AC power plugs and AC receptacles from water and other outdoor elements. You can accomplished by using a UL Listed waterproofing enclosure suitable for covering the AC receptacle and AC power plug that supplies power to the unit as described in Article 406 of the NEC.
3. When you install the access point outdoors or in a wet or damp location, the AC branch circuit that powers the access point should be provided with ground fault protection (GFCI), as required by Article 210 of the National Electrical Code (NEC).

Warning **Be very careful when connecting the streetlight adapter to Category 3 pole-top power. If you are not careful, you may electrocute yourself or fall.** Statement 363

Note For additional important safety instructions for AC power cords, refer to the *AC Power Cords for Cisco Aironet 1500 Series Outdoor Mesh Access Points* document that shipped with your AC power cords.

To install an access point on a light pole, follow these steps:

Step 1 When using the streetlight power tap adapter (AIR-PWR-ST-LT-TAP=), ensure that the access point is mounted within 3 ft (1m) of the outdoor light control. For mounting instructions, refer to the "Mounting the Access Point on a Pole" section on page 2-17.

Step 2 Refer to Figure 2-11. The streetlight power tap adapter uses a 3-pronged UL773 twist-lock adapter that is placed between the outdoor light control and its fixture. The UL773 twist-lock adapter is designed to be used with UL773 listed outdoor light controls operating at 100-to 240-VAC, 50/60 Hz.

Step 3 Disconnect the outdoor light control from its fixture.

Step 4 Verify that the voltage available at the fixture is between 100 and 240 VAC, 50/60 Hz.

Step 5 Turn off power to the fixture at the designated circuits.

Caution For your safety, when installing the streetlight power tap adapter to the access point AC power connector, always connect the access point end of the cable FIRST. When removing the streetlight power tap adapter, always disconnect the access point end of the cable LAST.

Warning **Use the captive connector cap on the unused mil spec connector to prevent water intrusion and possible safety hazards.** Statement 362

Step 6 Move the protective cap from the 5-pin AC power connector to the 12-pin Ethernet connector because the Ethernet connector is not used in light pole deployments.

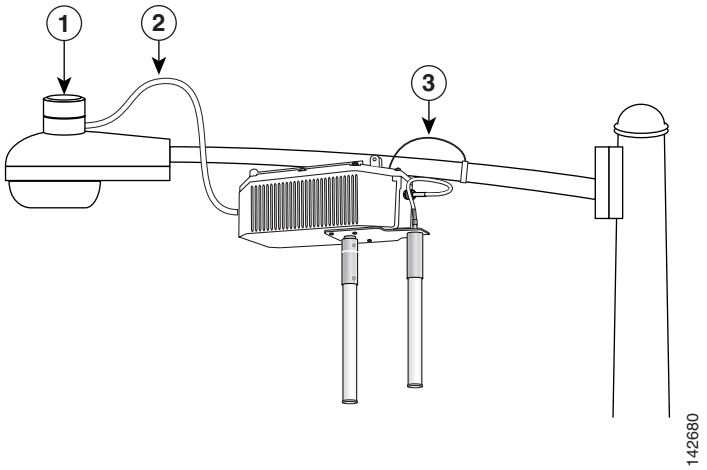
Note Ensure that your antennas are connected to the access point before you apply power to the access point.

Step 7 Connect the streetlight power tap adapter to the access point AC power connector, as shown in Figure 2-11.

Note Hand-tighten the cable connector until it locks. No specific torque is required.

Step 8 Plug the streetlight power tap adapter into the outdoor light control fixture, as shown in Figure 2-11.

Figure 2-11 Using the Streetlight Power Tap Adapter



1	Outdoor light control	**3**	10-AWG copper grounding wire
2	Streetlight power tap adapter		

Step 9 Plug the outdoor light control into the streetlight power tap adapter.

Step 10 Ensure the antennas are connected to the access point before you apply power to the access point.

Step 11 Turn on the power to the outdoor light control fixture at the designated circuits.

Note When you power up a MAP that is not connected to a wired Ethernet network to the controller, the access point uses the Cisco Adaptive Wireless Path Protocol to bind to another MAP with the best path to a RAP connected to the wired network to a controller.

The access point sends a discovery request when powered up. If you have configured the access point in the controller correctly, the controller sends back a discovery response to the access point. When that happens, the access point sends out a join request to the controller and the controller responds with a join confirmation response. Then, the access point establishes an LWAPP connection to the controller and gets the shared secret configured on the controller under zero-touch configuration.

What to Do Next

Refer to the *Cisco Wireless LAN Controller Configuration Guide* for more information on configuring, monitoring, and operating your access points. The following lists some of the configuration settings you might want to reconfigure:

- Changing the bridge shared secret key to a non-default value
- Selecting a backhaul channel when using the 4.9 MHz band (LAP1510 model only)
- Disabling the Zero Touch Configuration feature

CHAPTER 3

Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Sections in this chapter include:

Guidelines for Using the Access Points

You should keep these guidelines in mind when you use the access points:

- The access point can only communicate with controllers and cannot operate independently.
- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.
- The access points support Layer 2 or Layer 3 LWAPP communications with the controllers. In Layer 2 operation, the access point and the controller must be on the same subnet and communicate with each other using MAC addresses in encapsulated Ethernet frames. This operation is not scalable to larger networks and not recommended by Cisco.

  In Layer 3 operation, the access point and the controller can be on the same or different subnets. The access point communicates with the controller using standard IP packets. Layer 3 operation is scalable and is recommended by Cisco. A Layer 3 access point on a different subnet than the controller requires a DHCP server on the access point subnet and a route to the controller. The route to the controller must have destination UDP ports 12222 and 12223 open for LWAPP communications. The route to the primary, secondary, and tertiary controllers must allow IP packet fragments.
- Before deploying your access points ensure that the following has been done:
  - Your controllers are connected to switch ports that are configured as trunk ports.
  - Your access points are connected to switch ports that are configured as untagged access ports.
  - A DHCP server is reachable by your access points and has been configured with Option 43. Option 43 is used to provide the IP addresses of the Management Interfaces of your controllers. Typically, a DHCP server can be configured on a Cisco switch.
  - Optionally a DNS server can be configured to enable CISCO-LWAPP-CONTROLLER.<*local domain*> to resolve to the IP address of the Management Interface of your controller.
  - Your controllers are configured and reachable by the access points.
  - Your controllers are configured with the MAC addresses of the access points and Zero Touch Configuration is enabled.

Controller MAC Filter List

Prior to activating your access point, you must ensure that the access point MAC address has been added to the controller MAC Filter list. To view the MAC addresses added to the controller MAC filter list, you can use the controller CLI or the controller GUI:

- Controller CLI–Use the **show macfilter summary** controller CLI command to view the MAC addresses added to the controller filter list.
- Controller GUI–Log into your controller web interface (HTTPS) using a web browser and choose **SECURITY > MAC Filters** to view the MAC addresses added to the controller filter list.

Using DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling the access point to find and join a controller. Refer to the product documentation for your DHCP server for instructions on configuring DHCP Option 43. For additional information, refer to the "Configuring DHCP Option 43" section on page G-1.

Misconfigured Bridge Shared Secret Key

If an access point has a misconfigured bridge shared secret key, it is not allowed to join the mesh network. If **Enable Zero Touch Configuration** is checked on your controller, the access point can obtain the shared secret key from the controller or a neighbor access point.

If **Enable Zero Touch Configuration** is not checked, you might need to check the feature to allow the access point to get a new bridge shared secret key (refer to the "Enabling Zero Touch Configuration on the Controller" section on page 2-10).

Misconfigured MESH Access Point IP address

IP address misconfiguration can occur when you are re-addressing a segment of your mesh network and your first IP address change is the IP addresses of the RAP connected to the wired network. To avoid this problem, always start the IP addressing changes from the farthest access point and work your way back to the RAP. This problem might also happen if you move equipment; for example, you uninstall an access point and redeploy it in another physical location on the mesh network with a different IP subnet.

Another option to fix this misconfigured IP address is to physically take a controller in L2 mode with a RAP to the location of the misconfigured MAP. Set the bridge group name for the RAP to match the misconfigured MAP. Add the MAP's MAC address to the controller's filter list and check **Enable Zero Tough Configuration**. When the misconfigured MAP displays on the controller's Summary page, you can properly configure the access point.

Verifying Controller Association

To verify that your access point is associated to the controller, follow these steps:

Step 1 Log into your controller web interface (HTTPS) using a web browser.

Note You can also use the controller CLI **show ap summary** command from the controller console port.

Step 2 Click **Wireless** and verify that your access point MAC address is listed under Ethernet MAC.

Step 3 Logout of the controller and close your web browser.

Access Point Power

The access point does not have an LED to indicate available power.

Caution No serviceable parts inside. Do not open.

To ensure that your access point has power after installation, perform these steps:

Step 1 Ensure that the access point power source is turned-off.

Step 2 Remove and reconnect the AC power or Ethernet connector that supplies power to the access point.

Note Hand-tighten the connector until the connector locks.

Step 3 Ensure that all other cable connectors are properly connected.

Step 4 Turn-on the power source for the access point.

APPENDIX A

Translated Safety Warnings

For translated safety warnings, refer to the safety warning document that shipped with your access point or that is available on Cisco.com.

To browse to the document on Cisco.com, follow these steps:

Step 1 Click this link to the Cisco Wireless documentation home page:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Step 2 Click **Cisco Aironet 1500 Series** listed under Outdoor Wireless.

Step 3 Click **Install and Upgrade Guides**.

Step 4 Click **Translated Safety Warnings for Cisco Aironet 1500G Series Lightweight Outdoor Mesh Access Points**.

Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 1500 series lightweight outdoor mesh access point.

This appendix contains the following sections:

Manufacturers Federal Communication Commission Declaration of Conformity Statement

Model:

AIR-LAP1510AG-A-K9
AIR-LAP1505G-A-K9

FCC Certification number:

LDK102058

Manufacturer:

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician.

Caution The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using Cisco-supplied antennas. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

Caution To meet regulatory restrictions, the access point must be professionally installed.

Note The use of the 4.9-GHz band requires a license and may be used only by qualified Public Safety operators as defined in section 90.20 of the FCC rules (LAP1510 model only).

VCCI Statement for Japan

Warning **This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.**

警告 VCCI 準拠クラスB機器（日本）
この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

Industry Canada

IC Certification Number: 2461B-102058

Canadian Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur du Canada.

This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Cisco’s access points are certified to the requirements of RSS-210 issue 5, RSP 100, and RSS 102 for spread spectrum devices.

Declaration of Conformity for RF Exposure

This access point product has been found to be compliant to the requirements set forth in CFR 47 Section 1.1307 addressing RF Exposure from radio frequency devices as defined in Evaluating Compliance with FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields.T he antennas should be positioned more than 6.56 feet (2 meters) from your body or nearby persons.

This access point is also compliant to EN 50835 for RF exposure.

Administrative Rules for Cisco Aironet Access Points in Taiwan

This section provides administrative rules for operating Cisco Aironet access points in Taiwan. The rules are provided in both Chinese and English.

Chinese Translation

低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

127048

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 12

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

Article 14

The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with the Communication Act.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

Operation of Cisco Aironet Access Points in Brazil

This section contains special information for operation of Cisco Aironet access points in Brazil.

Access Point Models

AIR-LAP1510G-A-K9
AIR-LAP1505G-A-K9

Regulatory Information

Figure 1-1 contains Brazil regulatory information for the AIR-LAP1510G-A-K9 and the AIR-LAP1505G-A-K9 access points.

Figure 1-1 Brazil Regulatory Information

Portuguese Translation

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

English Translation

This equipment operates on a secondary basis and consequently must accept harmful interference, including interference from stations of the same kind. This equipment may not cause harmful interference to systems operating on a primary basis.

APPENDIX C

Access Point Specifications

Table C-1 lists the technical specifications for the Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Point.

Table C-1 Access Point Specifications

Category	Specifications		
	802.11b	**802.11g**	**802.11a (LAP1510 model)**
Size	15.0 in x 7.3 in x 5.7 in. (38.1 cm x 18.5 cm x 14.5 cm) (includes antenna mount bracket)		
Connectors	Ethernet (POE) connector—12 pin circular Mil spec (MS3112P14-12P) AC power connector—5 pin circular Mil spec (MS3112P14-5P) 2.4-GHz Type N antenna connector 5-GHz Type N antenna connector—(LAP1510 model)		
Input voltage	100- to 240- VAC, 50/60 Hz (nominal) 48 VDC (nominal)		
Input power	DC inline PoE power 28.5 W at 48 VDC (nominal) AC power 57.8 W at 120 VAC (nominal) 70.3 W at 240 VAC (nominal)		
Operating temperature	Access point –40 to 131°F (–40 to 55°C) Power injector 30 to 140°F (0 to 60°C)		
Storage temperature	Access point –58 to 185°F (–50 to 85°C) Power injector -76 to 158°F (-60 to 70°C)		
Weight	10 lbs. (4.55 kg)		
Modulation	Complementary Code Keying (CCK)	Orthogonal Frequency Division Multiplex (OFDM)	

Table C-1 Access Point Specifications (continued)

Category	Specifications		
	802.11b	**802.11g**	**802.11a (LAP1510 model)**
Subcarrier modulation	BPSK (1 Mbps) QPSK (2 Mbps) CCK (5.5 and 11 Mbps)	BPSK (6 and 9 Mbps) QPSK (12 and 18 Mbps) 16-QAM (24 and 36 Mbps) 64-QAM (48 and 54 Mbps)	BPSK (6 Mbps and 9 Mbps) QPSK (12 Mbps and 18 Mbps) 16-QAM (24 and 36 Mbps) 64-QAM (48 and 54 Mbps)
Power output	**CCK**	**OFDM**	**OFDM**
	24 dBm conducted		26 dBm conducted
	Maximum output depends on the regulatory domain in which the access point is installed. For additional information, refer to the Channels and Power Levels section.		
Frequency	2.400 to 2.484 GHz		4.940 to 4.990 GHz [1] 5.470 to 5.725 GHz 5.725 to 5.85 GHz
	Frequency depends on the regulatory domain in which the access point is installed. For additional information, refer to the Channels and Power Levels section.		
Data rates	1, 2, 5.5, and 11 Mbps	6, 9, 12, 18, 24, 36, 48, and 54 Mbps	
Environmental ratings	NEMA Type 4X, IP66		
Maximum elevation	6561 ft (2000 m)		
Wind resistance	Up to 165 MPH		
Immunity	Less than or equal to 5 mJ for 6kV/3kA @ 8/20 ms waveform ANSI/IEEE C62.41 EN61000-4-5 Level 4 AC Surge Immunity EN61000-4-4 Level 4 Electrical Fast Transient Burst Immunity EN61000-4-3 Level 4 EMC Field Immunity EN61000-4-2 Level 4 ESD Immunity		
Safety	Designed to meet: AS/NZS 60950.1 IEC 60950-1 UL 60950-1 CSA 60950-1 EN 60950-1 IEC60664-1 Overvoltage category IV (for streetlight installations)		
Radio approvals	FCC Parts 15.247, 90.210 FCC Bulletin OET-65C Canada RSS-210 and RSS-102 AS/NZS 4268.2003		
EMI and Susceptibility	FCC Part 15.107 and 15.109 ICES-003 (Canada) EN 55022 EN 55022		

1. The use of the 4.9-GHz band requires a license and may be used only by qualified Public Safety operators as defined in section 90.20 of the FCC rules.

APPENDIX D

Channels and Power Levels

For channel and maximum power level settings, refer to the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points and Bridges* document available on the Cisco Wireless documentation page of Cisco.com.

To browse to the document, follow these steps:

Step 1 Click this link to the Cisco Wireless documentation home page:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Step 2 Click **Cisco Aironet 1500 Series** listed under Outdoor Wireless.

Step 3 Click **Install and Upgrade Guides**.

Step 4 Click **Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points and Bridges**.

APPENDIX E

Connector Pinouts

This appendix describes the pin signals of the access point AC power connector (MS3112P14-5P), the access point Ethernet (POE) connector (MS3112P14-12P), and the power injector Input and Output connectors. Table E-1 describes the pin signals of the AC power connector.

Table E-1 AC Power Connector (MS3112P14-5P) Pinouts

Pin Number	Signal Name
A	Neutral
B	Line
C	(unused)
D	Case Ground
E	(unused)

Table E-2 describes the pin signals of the Ethernet (POE) connector.

Table E-2 Ethernet (POE) Connector (MS3112P14-12P) Pinouts

Pin Number	Signal Name
A	Ethernet Tx+
B	Ethernet Tx–
C	Ethernet Rx+
D	Ethernet Rx–
E	RS232 TxD[1]
F	RS232 RxD[1]
G	Ground Signal/RS232
H	(unused)
J	(unused)
K	Case Ground
L	DC+ (the DC power goes through a bridge rectifier, so polarity should not be an issue)
M	DC- (this side of the DC power is fused)

1. Not used in the access point outdoor Ethernet cable (AIR-ETH1500-150=).

Table E-3 describes the pin signals for the power injector Input connector (RJ-45).

Table E-3 Power Injector Input Connector Pinouts

Pin Number	Signal Name
1	Ethernet Tx+
2	Ethernet Tx–
3	Ethernet Rx+
4	(unused)
5	(unused)
6	Ethernet Rx–
7	(unused)
8	(unused)

Table E-4 describes the pin signals for the power injector Output connector (RJ-45).

Table E-4 Power Injector Output Connector Pinouts

Pin Number	Signal Name
1	Ethernet Tx+
2	Ethernet Tx–
3	Ethernet Rx+
4	48 VDC power (+)
5	48 VDC power (+)
6	Ethernet Rx–
7	48 VDC power (return)
8	48 VDC power (return)

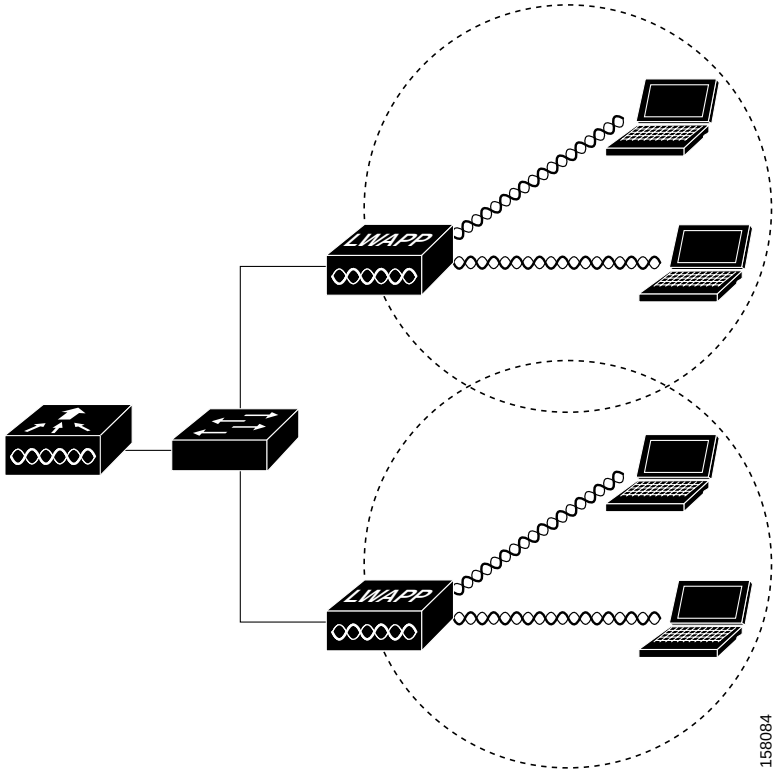
APPENDIX F

Priming Access Points Prior to Deployment

This section describes an optional procedure designed to prime or stage your access points in a convenient location rather than after they are installed in possibly difficult to reach locations. This helps limit potential installation problems to primarily Ethernet and power areas.

Figure F-1 illustrates a typical priming configuration for your access points.

Figure F-1 Typical Priming Configuration



Before deploying your access points to their final locations, follow these steps to prime your access points:

Step 1 Use the controller CLI, controller GUI, or Cisco WCS to configure your controller:

a. Add the MAC addresses of your access points in controller filter list (refer to the "Adding the Access Point MAC Addresses to the Controller Filter List" section on page 2-10).

b. Enable Zero Touch Configuration on your controller (refer to the "Enabling Zero Touch Configuration on the Controller" section on page 2-10).

Step 2 In a Layer 2 environment, where the access points are located on the same subnet as the controller, the access point communicates directly with the controller. In this environment, you don't need a DHCP server on the same subnet as the access points because the access points receive IP address information from the controller.

Step 3 In a Layer 3 environment, ensure that a DHCP server (typically on your switch) is enabled on the same subnet as your access points. The access points will receive its IP address and controller information using DHCP Option 43.

The access point must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, OTAP, or IP subnet broadcast. This guide describes the DHCP method to convey the controller IP address. For other methods, refer to the product documentation. Refer to the "Controller MAC Filter List" section on page 3-2 for more information.

Note For a Layer 3 access point on a different subnet than the controller, ensure that the route to the controller has destination UDP ports 12222 and 12223 open for LWAPP communications. Ensure that the routes to the primary, secondary, and tertiary controllers allow IP packet fragments.

Step 4 Ensure that your controller is connected to a switch trunk port.

Step 5 Configure the controller in LWAPP Layer 3 mode and ensure that its DS Port is connected to the switch. Use the CLI, web-browser interface, or Cisco WCS procedures as described in the appropriate controller guide.

a. In multi-controller environments, You can set one controller's DS port to **Master** (you can use the *config network master-base disable* CLI command or you can use the controller GUI*)* so that new access points always associate with it. You can use the **show network config** CLI command to determine if the controller DS port is the master.

All access points associate to the master controller. From one location, you can configure access point settings such as primary, secondary, and tertiary controllers. This allows you to redistribute your access points to other controllers on the network.

You can also use a Cisco WCS server to control, configure, and redistribute all your access points from a single location.

Step 6 Apply power to the access points:

a. Connect your access points to untagged access ports on your POE capable switch. You can optionally use power injectors (AIR-PWRINJ1500=) to power your access points.

b. When the access point associates with the controller, if the access point code version differs from the controller code version, the access point downloads the operating system code from the controller.

c. When the operating system download is successful, the access point reboots.

Step 7 Use the controller CLI, controller GUI, or Cisco WCS to configure the access point with primary, secondary, and tertiary controller names.

Step 8 If the access point is in a Controller Mobility Group, use the controller CLI, controller GUI, or Cisco WCS to configure the Controller Mobility Group name.

Step 9 Use controller CLI, controller GUI, or Cisco WCS to configure the access point-specific 802.11a, 802.11b, and 802.11g network settings.

Step 10 Repeat Steps 4 to 9 for each access point.

When you successfully complete the configuration priming of all your access points, ensure that Master setting is disabled on your controller. You can begin deploying the access points to their final destinations.

APPENDIX G

Configuring DHCP Option 43

This appendix describes the steps needed to configure DHCP Option 43 on a Windows 2003 Enterprise DHCP server, such as a Cisco Catalyst 3750 series switch, for use with Cisco Aironet lightweight access points. This appendix contains these sections:

Overview

This section contains a DHCP Option 43 configuration example on a Windows 2003 Enterprise DHCP server for use with Cisco Aironet lightweight access points. For other DHCP server implementations, consult DHCP server product documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.

Note DHCP Option 43 is limited to one access point type per DHCP pool. You must configure a separate DHCP pool for each access point type.

Cisco Aironet 1000 and 1500 series access points use a comma-separated string format for DHCP Option 43. Other Cisco Aironet access points use the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP Option 60). The VCI strings for Cisco access points capable of operating in lightweight mode are listed in Table G-1:

Table G-1 Lightweight Access Point VCI Strings

Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	Airespace AP1200
Cisco Aironet 1100 series	Cisco AP c1100
Cisco Aironet 1130 series	Cisco AP c1130
Cisco Aironet 1200 series	Cisco AP c1200
Cisco Aironet 1240 series	Cisco AP c1240
Cisco Aironet 1300 series	Cisco AP c1300
Cisco Aironet 1500 series	Cisco AP c1500[1]
	Cisco AP OAP1500[2], Cisco AP LAP1510[2], or Cisco AP LAP1505[2]
	Airespace AP1200[3]

1. For controller release 4.1 or later.
2. For controller release 4.0, the VCI depends on the model.
3. For controller release 3.2

The format of the TLV block for 1100, 1130, 1200, 1240, 1250, and 1300 series access points is listed below:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of WLC management interfaces

Configuring Option 43 for 1000 Series Access Points

To configure DHCP Option 43 for Cisco 1000 series lightweight access points in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS command line interface (CLI).

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>

Where:
    <pool name> is the name of the DHCP pool, such as AP1000
    <IP Network> is the network IP address where the controller resides, such as 10.0.15.1
    <Netmask> is the subnet mask, such as 255.255.255.0
    <Default router> is the IP address of the default router, such as 10.0.0.1
    <DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 60 line using the following syntax:

```
option 60 ascii "Airespace.AP1200"
```

The quotation marks must be included.

Step 4 Add the option 43 line using the following syntax:

```
option 43 ascii "Comma Separated IP Address List"
```

For example, if you are configuring option 43 for Cisco 1000 series access points using the controller IP addresses 10.126.126.2 and 10.127.127.2, add the following line to the DHCP pool in the Cisco IOS CLI:

```
option 43 ascii "10.126.126.2,10.127.127.2"
```

The quotation marks must be included.

Configuring Option 43 for 1100, 1130, 1200, 1240, and 1300 Series Access Points

To configure DHCP Option 43 for Cisco Aironet 1100, 1130, 1200, 1240, and 1300 series lightweight access points in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS CLI.

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>

Where:
    <pool name> is the name of the DHCP pool, such as AP1240
    <IP Network> is the network IP address where the controller resides, such as 10.0.15.1
    <Netmask> is the subnet mask, such as 255.255.255.0
    <Default router> is the IP address of the default router, such as 10.0.0.1
    <DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 60 line using the following syntax:

option 60 ascii "*VCI string***"**

For the *VCI string*, use the value from Table G-1. The quotation marks must be included.

Step 4 Add the option 43 line using the following syntax:

option 43 hex *<hex string>*

The *hex string* is assembled by concatenating the TLV values shown below:

Type + Length + Value

Type is always *f1(hex)*. *Length* is the number of controller management IP addresses times 4 in hex. *Value* is the IP address of the controller listed sequentially in hex.

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is *f1(hex)*. The length is *2 * 4 = 8 = 08 (hex)*. The IP addresses translate to *0a7e7e02* and *0a7f7f02*. Assembling the string then yields *f1080a7e7e020a7f7f02*. The resulting Cisco IOS command added to the DHCP scope is listed below:

```
option 43 hex f1080a7e7e020a7f7f02
```

Configuring Option 43 for 1500 Series Access Points

To configure DHCP Option 43 for Cisco 1500 series lightweight access points in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS command line interface (CLI).

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>

Where:
    <pool name> is the name of the DHCP pool, such as AP1500
    <IP Network> is the network IP address where the controller resides, such as 10.0.15.1
    <Netmask> is the subnet mask, such as 255.255.255.0
    <Default router> is the IP address of the default router, such as 10.0.0.1
    <DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 60 line using the following syntax:

```
option 60 ascii "Cisco AP c1500"
```

The quotation marks must be included.

Step 4 Add the option 43 line using the following syntax:

```
option 43 ascii "Comma Separated IP Address List"
```

For example, if you are configuring option 43 for Cisco 1500 series access points using the controller IP addresses 10.126.126.2 and 10.127.127.2, add the following line to the DHCP pool in the Cisco IOS CLI:

```
option 43 ascii "10.126.126.2,10.127.127.2"
```

The quotation marks must be included.

INDEX

I

L

M

N

O

P

R

S

T

U

V

W

Z